(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10198776 A**

(43) Date of publication of application: **31.07.98**

(51) Int. Cl **G06K 19/07**
G06K 17/00
G06K 19/10

(21) Application number: **09017427**

(22) Date of filing: **14.01.97**

(71) Applicant: **DAINIPPON PRINTING CO LTD**

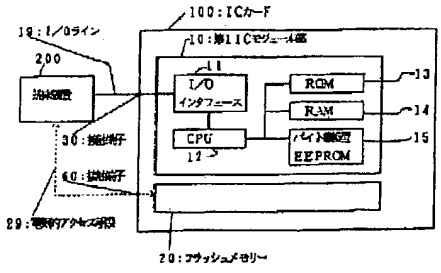
(72) Inventor: **ISHIBASHI MASAKAZU**

(54) **PORTABLE INFORMATION RECORDING MEDIUM, AND ITS INFORMATION WRITING AND READING METHOD**

(57) Abstract:

PROBLEM TO BE SOLVED: To make it possible to record a large amount of information, and also to improve the processing speed and security of a portable information recording medium, by recording the information to both 1st and 2nd IC modules containing the nonvolatile memories.

SOLUTION: An IC card 100 serves as a double chip type IC card, which contains a 1st IC module part 10 and a flash erasion type EEPROM (flash memory) 20 that is formed on the card surface as a 2nd IC module part. A contact terminal 30 is provided on the surface of the part 10. The card 100 is accessed by an exclusive terminal equipment 200. For instance, a byte rewrite type EEPROM 15 included in the part 10 of the card 100 has the memory capacity of only 8KB. On the other hand, the memory 20 can record the information of 8MB. Therefore, the card 100 can record a large quantity of information compared with an IC card provided with only the module part 10.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－198776

(43)公開日　平成10年(1998)７月31日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｋ 19/07		Ｇ０６Ｋ 19/00	Ｎ
17/00		17/00	Ｔ
19/10		19/00	Ｒ

審査請求　未請求　請求項の数10　ＦＤ　（全 15 頁）

(21)出願番号　特願平9－17427

(22)出願日　平成９年(1997)１月14日

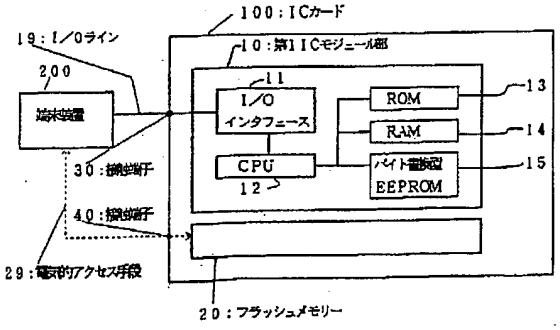
(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　石橋　正教
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(74)代理人　弁理士　小西　淳美

(54)【発明の名称】　携帯可能情報記録媒体およびこれに対する情報書込／読出方法

(57)【要約】

【課題】　２つのＩＣモジュールに情報を記録することにより大容量の情報記録が可能で、処理速度の速い携帯可能情報記録媒体を提供し、かつ、セキュリティが非常に高く、情報の改ざんに対処する。

【解決手段】　ＣＰＵと、このＣＰＵが実行するプログラムを記憶したＲＯＭと、ＣＰＵの作業領域として使用されるＲＡＭと、ＣＰＵを介してデータの読出しおよび書き込みができる電気的に消去・再書き込み可能な不揮発性メモリと、を有する第一ＩＣモジュールと、電気的に消去・再書き込み可能な不揮発性メモリからなる第二ＩＣモジュールと、を搭載し、第一ＩＣモジュール内と第二ＩＣモジュール内との双方に情報記録を行うことができる携帯可能情報記録媒体である。



1

【特許請求の範囲】

【請求項１】　ＣＰＵと、このＣＰＵが実行するプログラムを記憶したＲＯＭと、前記ＣＰＵの作業領域として使用されるＲＡＭと、前記ＣＰＵを介してデータの読出しおよび書き込みができる電気的に消去・再書き込み可能な不揮発性メモリと、を有する第一ＩＣモジュールと、

電気的に消去・再書き込み可能な不揮発性メモリからなる第二ＩＣモジュールと、を搭載し、

前記第一ＩＣモジュール内と前記第二ＩＣモジュール内との双方に情報記録を行うことができる携帯可能情報記録媒体。

【請求項２】　前記第一ＩＣモジュール内の不揮発性メモリがバイト書換型ＥＥＰＲＯＭであり、前記第二ＩＣモジュール内の不揮発性メモリがフラッシュ消去型ＥＥＰＲＯＭであることを特徴とする請求項１記載の携帯可能情報記録媒体。

【請求項３】　前記第一ＩＣモジュール内に対して外部から所定のデータが与えられたときに、前記第一ＩＣモジュール内の不揮発性メモリ内に記録されている暗号化キーを用いて、前記データから一義的に導出される認証コードを生成する認証コード生成処理を前記ＣＰＵが実行できるように、認証コード生成プログラムを前記ＲＯＭ内に用意したことを特徴とする請求項１、２記載の携帯可能情報記録媒体。

【請求項４】　請求項３に記載の媒体において、

与えられたデータをｎ個（ｎ≧２）のブロックに分割し、このｎ個のブロックにｍ個の暗号化キー（ｍ≧１）を加えた（ｎ＋ｍ）組のデータのすべてが関与した相互論理演算を行い、前記与えられたデータのデータ長よりも短い認証コードを生成することができる認証コード生成プログラムを用意したことを特徴とする携帯可能情報記録媒体。

【請求項５】　請求項３または４に記載の媒体において、

第一ＩＣモジュール内で生成された認証コードを、この認証コードのもととなったデータに付加して、第二ＩＣモジュール内に記録したことを特徴とする携帯可能情報記録媒体。

【請求項６】　請求項３～５のいずれかに記載の媒体において、

第一ＩＣモジュールに接続されている端末装置が正規のものであるか否かを判定する機能を第一ＩＣモジュールに用意し、正規の端末装置であった場合にのみ、認証コード生成処理が実行されるようにしたことを特徴とする携帯可能情報記録媒体。

【請求項７】　ＣＰＵと、このＣＰＵによってアクセスされる第一メモリと、電気的に消去・再書き込み可能な不揮発性メモリからなる第二メモリとを有し、前記第一メモリと前記第二メモリとの双方に情報記録を行うことができる携帯可能情報記録媒体に対する情報書込方法であって、

2

前記第二メモリへ書込むべき記録対象データを用意し、

前記第一メモリ内に記録されている暗号化キーを用いて、前記記録データから一義的に導出される認証コードを生成する認証コード生成処理を前記ＣＰＵによって実行させ、

生成された認証コードを前記記録対象データに付加して前記第二メモリへ書込むようにしたことを特徴とする携帯可能情報記録媒体に対する情報書込方法。

【請求項８】　請求項７に記載の情報書込方法において、

第二メモリに記録されている暗号化キーを、この媒体に接続されている端末装置についてのホストコンピュータ内にも用意し、認証コード生成処理を前記媒体内のＣＰＵに実行させる代わりに、前記ホストコンピュータに実行させることを特徴とする携帯可能情報記録媒体に対する情報書込方法。

【請求項９】　請求項７または８に記載の方法によって第二メモリに書込まれた情報を読み出す方法であって、

第二メモリに書込まれている記録対象データおよび認証コードを読出し、媒体の第一メモリ内に記録されている暗号化キーを用いて、前記記録対象データから一義的に導出される認証コードを生成する認証コード生成処理を前記ＣＰＵによって実行させ、

第二メモリから読み出された認証コードと、前記認証コード生成処理で生成された認証コードとを比較し、両者が一致している場合にのみ、第二メモリから読み出された記録対象データを正しいデータとして取り扱うことを特徴とする携帯可能情報記録媒体に対する情報読出方法。

【請求項１０】　請求項９に記載の情報読出方法において、

第二メモリ内に記録されている暗号化キーを、この媒体に接続されている端末装置についてのホストコンピュータ内にも用意し、認証コード生成処理を前記媒体内のＣＰＵに実行させる代わりに、前記ホストコンピュータに実行させることを特徴とする携帯可能情報記録媒体に対する情報読出方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は携帯可能情報記録媒体およびこれに対する情報書込／読出方法に関し、特にＣＰＵとメモリを有するＩＣモジュールを１つ目とし、電気的に消去・再書き込み可能な不揮発性メモリからなるＩＣモジュールを２つ目として搭載された、いわゆる２チップ型のＩＣカードなどに対して利用するのに適した情報の書込／読出方法に関する。

【０００２】

【従来の技術】携帯可能情報記録媒体として、現在、磁

気カードが広く普及しているが、大きな記憶容量を確保できる光カードや十分なセキュリティを確保できるＩＣカードも実用化されている。今後は、半導体集積回路の小型化、低コスト化のための技術進歩により、実社会の種々のシステムにおいてＩＣカードが利用されるものと思われる。

【０００３】特に、ＣＰＵを内蔵したＩＣカードでは、単なる情報記録媒体としての機能だけではなく、情報処理機能が付加されるため、高度なセキュリティを必要とする情報処理システムへの利用が期待されている。現在普及している一般的なＩＣカードは、ＣＰＵと、このＣＰＵによってアクセスされる３種類のメモリ、すなわち、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭを有している。ＲＯＭ内には、ＣＰＵによって直接実行可能なインストラクションコードからなるプログラムが記憶されており、ＣＰＵはこのプログラムに基づいて、ＩＣカードを統括制御する機能を有する。ＲＡＭは、ＣＰＵがこのような統括制御を行う上での作業領域として使用されるメモリである。一方、ＥＥＰＲＯＭは、ＣＰＵを介してデータの読出しおよび書き込みが可能な不揮発性メモリであり、このＩＣカードに記録すべき本来のデータを格納するために用いられる。

【０００４】光カードでは、表面に情報記録部が設けられており、光学的読取装置を用いることにより、この情報記録部に記録されたデジタルデータを読み取ることが可能である。このため、不正な手段による読出しも比較的容易に行いうる。これに対して、ＩＣカードに内蔵されているＥＥＰＲＯＭへのアクセスは、すべてＣＰＵを介して行われ、外部からＥＥＰＲＯＭを直接アクセスすることはできない。したがって、ＩＣカードは、光カードに比べて高度なセキュリティを確保することが可能になる。そこでＩＣメモリによる記録と、光記録、光磁気記録などの光を用いた記録とを併用したいわゆる「ハイブリッド型」の情報記録カードが提案されている。

【０００５】たとえば、光記録を併用したハイブリッドＩＣカードでは、カード状の媒体内部にＩＣモジュールが埋め込まれるとともに、表面に光記録部が形成される。このようなハイブリッドＩＣカードを用いれば、記録すべき情報は、ＩＣモジュール内のＥＥＰＲＯＭへデジタルデータとして記録することもできるし、光記録部にデジタルピットとして記録することもできる。そこで、高度なセキュリティを要する情報についてはＥＥＰＲＯＭへ記録し、大容量の情報については光記録部へ記録する、という利用形態が可能となる。

【０００６】

【発明が解決しようとする課題】しかし、上述したハイブリッドＩＣカードでは、光記録部へ大容量の情報を記録することが可能になるが、光記録部は、その書き込みや読み取りにおいて、カードの上下あるいは左右の方向に直線状にしか記録できず、したがって光学的読取装置

の読取り部を上下あるいは左右方向に往復動することでしか書き込みや読み取りができないものであり、処理速度が遅く、時間を非常に要し、かつリーダライターをコンパクトにできないものであった。また、その記録に関しても追記のみであり、書換えが不可能なもので、かつ表面に傷などがつき易い等の欠点も有するものであった

【０００７】また、光記録部に記録された情報に対するセキュリティは低いものであり、そこで、秘密にする必要性の低い情報を光記録部へ記録するのが一般的な利用形態となる。すなわち、万一、不正な手段によって読み取られることがあっても、重大な事態にはならないような情報を光記録部へ記録するようにすれば、不正読み取りによるセキュリティ上の大きな問題は解決できる。ところが、不正な手段による書き込みが行われると、利用上、大きな問題が生じることになる。すなわち、不正書き込みを行えば、記録データを改ざんすることが可能であり、このようなデータ改ざんが行われると、ＩＣカードを利用した運用システム全体に大きな支障を生じる可能性がある。光記録部に記録された情報は、微小なデータピットの有無によってＩビットを表現した情報であり、新たなデータピットを生成することにより比較的容易に改ざんが可能である。光磁気記録部に記録された情報も同様に改ざんされる可能性がある。

【０００８】そこで本発明は、ＣＰＵを有するＩＣモジュールと、それ以外のカード表面に電気的に消去・再書き込み可能な不揮発性メモリからなる別のＩＣモジュールとを搭載し、その双方のＩＣモジュールに情報を記録することのできる、大容量の情報記録が可能で、処理速度の速い携帯可能情報記録媒体を提供するとともに、その記録情報に対するセキュリティの非常に高い、情報記録部に記録された情報の改ざんに対処することを目的とする。

【０００９】

【課題を解決するための手段】

(1) 本発明の第１の態様は、ＣＰＵと、このＣＰＵが実行するプログラムを記憶したＲＯＭと、ＣＰＵの作業領域として使用されるＲＡＭと、ＣＰＵを介してデータの読出しおよび書き込みができる電気的に消去・再書き込み可能な不揮発性メモリと、を有する第一ＩＣモジュールと、電気的に消去・再書き込み可能な不揮発性メモリからなる第二ＩＣモジュールと、を搭載し第一ＩＣモジュール内と第二ＩＣモジュール内との双方に情報記録を行うことができる携帯可能情報記録媒体である。

【００１０】(2) 本発明の第２の態様は、第一ＩＣモジュール内の不揮発性メモリがバイト書換型ＥＥＰＲＯＭであり、第二ＩＣモジュールの不揮発性メモリがフラッシュ消去型ＥＥＰＲＯＭであることを特徴とするものである。

【００１１】(3) 本発明の第３の態様は、第一ＩＣモジュール内に対して外部から所定のデータが与えられたと

きに、第一ＩＣモジュール内の不揮発性メモリ内に記録されている暗号化キーを用いて、データから一義的に導出される認証コードを生成する認証コード生成処理をＣＰＵが実行できるように、認証コード生成プログラムをＲＯＭ内に用意したものである。

【００１２】(4) 本発明の第４の態様は、上述の第３の態様に係る携帯可能情報記録媒体において、与えられたデータをｎ個（ｎ≧２）のブロックに分割し、このｎ個のブロックにｍ個の暗号化キー（ｍ≧１）を加えた（ｎ＋ｍ）組のデータのすべてが関与した相互論理演算を行い、前記与えられたデータのデータ長よりも短い認証コードを生成することができるようにしたものである。

【００１３】(5) 本発明の第５の態様は、上述の第３または第４の態様に係る携帯可能情報記録媒体において、第一ＩＣモジュール内で生成された認証コードを、この認証コードのもととなったデータに付加して、第二ＩＣモジュール内に記録したものである。

【００１４】(6) 本発明の第６の態様は、上述の第３～５の態様に係る携帯可能情報記録媒体において、第一ＩＣモジュールに接続されている端末装置が正規のものであるか否かを判定する機能を第一ＩＣモジュールに用意し、正規の端末装置であった場合にのみ、認証コード生成処理が実行されるようにしたものである。

【００１５】(7) 本発明の第７の態様は、ＣＰＵと、このＣＰＵによってアクセスされる第一メモリと、電気的に消去・再書き込み可能な不揮発性メモリからなる第二メモリとを有し、第一メモリと第二メモリとの双方に情報記録を行うことができる携帯可能情報記録媒体に対する情報書込方法であって、第二メモリへ書込むべき記録対象データを用意し、第一メモリ内に記録されている暗号化キーを用いて、記録データから一義的に導出される認証コードを生成する認証コード生成処理をＣＰＵによって実行させ、生成された認証コードを記録対象データに付加して第二メモリへ書込むようにしたものである。

【００１６】(8) 本発明の第８の態様は、上述の第７の態様に係る携帯可能情報記録媒体に対する情報書込方法において、第二メモリに記録されている暗号化キーを、この媒体に接続されている端末装置についてのホストコンピュータ内にも用意し、認証コード生成処理を媒体内のＣＰＵに実行させる代わりに、ホストコンピュータに実行させるようにしたものである。

【００１７】(9) 本発明の第９の態様は、上述の第７または第８の態様に係る方法によって情報記録部に書込まれた情報を読み出す方法において、第二メモリに書込まれている記録対象データおよび認証コードを読出し、媒体の第一メモリ内に記録されている暗号化キーを用いて、記録対象データから一義的に導出される認証コードを生成する認証コード生成処理を前記ＣＰＵによって実行させ、第二メモリから読み出された認証コードと、認証コード生成処理で生成された認証コードとを比較し、

両者が一致している場合にのみ、第二メモリから読み出された記録対象データを正しいデータとして取り扱うようにしたものである。

【００１８】(10) 本発明の第１０の態様は、上述の第９の態様に係る携帯可能情報記録媒体に対する情報読出方法において、情報記録部内に記録されている暗号化キーを、この媒体に接続されている端末装置についてのホストコンピュータ内にも用意し、認証コード生成処理を前記媒体内のＣＰＵに実行させる代わりに、ホストコンピュータに実行させるようにしたものである。

【００１９】そこで本発明は、ＣＰＵを有するＩＣモジュールと、それ以外のカード表面に電気的に消去・再書き込み可能な不揮発性メモリからなる別のＩＣモジュールとを搭載し、その双方のＩＣモジュールに情報を記録することのできる、大容量の情報記録が可能で、処理速度が速く、かつ表面物性に優れた携帯可能情報記録媒体を提供するとともに、その記録情報に対するセキュリティの非常に高い、電気的に消去・再書き込み可能な不揮発性メモリからなるＩＣモジュールに記録された情報の改ざんに対処することを目的とする。

【００２０】

【作用】本発明に係る携帯可能情報記録媒体では、ＣＰＵを有するＩＣモジュールと、それ以外のカード表面に電気的に消去・再書き込み可能な不揮発性メモリからなる別のＩＣモジュールとの双方に情報を記録することができるので、大容量の情報記録を可能とし、処理速度においても非常に速く、表面物性に優れたものとすることができる。

【００２１】また、ＣＰＵを有する第一ＩＣモジュールのメモリに、暗号化キーが用意され、内蔵ＣＰＵによってこの暗号化キーを用いた認証コード生成処理を実行する機能が付加されている。そこで、電気的に消去・再書き込み可能な不揮発性メモリからなる第二ＩＣモジュールへ記録すべきデータに対して認証コードを生成し、生成した認証コードをもとのデータに付加した状態で書込みを行えば、読出し時には、この認証コードの整合性をチェックすることにより、データに対する改ざんの有無を認識することができる。

【００２２】たとえば、２チップ型ＩＣカードの表面の電気的に消去・再書き込み可能な不揮発性メモリからなる第二ＩＣモジュールにデータＤを書込む場合は、このデータＤに対して、第二ＩＣモジュール内で所定の暗号化キーを用いた認証コード生成処理を実行し、認証コードＣを生成する。そして、データＤに認証コードＣを付加した形で、第二ＩＣモジュールに書込みを行う。一方、読出し時には、データＤとともにコードＣを読出し、このデータＤと暗号化キーとに基づいて生成した認証コードと、読出したコードＣとが一致するか否かをチェックすればよい。第二ＩＣモジュールに対する改ざんが行われていた場合には、このチェックにより不一致が

生じるため、改ざんを認識することができる。認証コード生成処理に用いられる暗号化キーは、ＣＰＵを有する第一ＩＣモジュール内に記録されているため、不正な手段によってこの暗号化キーを外部へ読み出すことは非常に困難であり、不正な手段によって認証コードが生成される可能性は極めて低い。

【００２３】もっとも、暗号化キーに対するセキュリティが十分に確保できる環境においては、暗号化キーを媒体の外部に用意し、認証コード生成処理を外部で行うことも可能である。たとえば、媒体をアクセスするための端末装置に接続されたホストコンピュータについて十分なセキュリティが得られるのであれば、このホストコンピュータ内に暗号化キーを用意して認証コード生成処理を実行できるようにしておけば、この認証コード生成処理をより短時間で実行できるメリットが得られる。

【００２４】また、媒体の内部で認証コード生成処理を実行する場合、ＣＰＵを有する第一ＩＣモジュールに接続されている端末装置が正規のものであるか否かを判定し、正規の端末装置で合った場合にのみ、認証コード生成処理が実行されるようにしておけば、セキュリティを更に向上させることができる。

【００２５】

【発明の実施の形態】以下、本発明を図示する実施例に基づいて説明する。

【００２６】§１．２チップ型ＩＣカードの構成

はじめに、２チップ型ＩＣカードの構成を説明する。図１に外観を示すＩＣカード１００は、第一ＩＣモジュール部１０を内蔵し、表面に第二ＩＣモジュール部としてフラッシュ消去型ＥＥＰＲＯＭ２０（以下、フラッシュメモリー２０という）が形成された２チップ型ＩＣカードである。第一ＩＣモジュール部１０の表面には、接触端子３０が設けられている。このＩＣカード１００に対するアクセスは、専用の端末装置２００によって行われる。端末装置２００にＩＣカード１００を挿入すると、端末装置２００内の電極と接触端子３０とが電気的に接触し、この接触端子３０を介して、第一ＩＣモジュール部１０に対する電源供給、クロック供給、データの送受が行われることになる。また、端末装置２００には、フラッシュメモリー２０の表面に設けられた接触端子４０を介して上記同様に電気的に書き込んだり、フラッシュメモリー２０内に電気的に記録されている領域の情報を読み込んだりする電気的アクセス手段が組み込まれている。

【００２７】図２は、このＩＣカード１００を端末装置２００に接続し、アクセスを行っている状態を示すブロック図である。ＩＣカード１００と端末装置２００とはＩ／Ｏライン１９および接触端子３０を介して相互に接続されている。この他、端末装置２００とＩＣカード１００との間には、電源・クロック・リセット信号などの供給路が形成されるが、ここではこれら供給路の図示は省略する。

【００２８】ＩＣカード１００に内蔵された第一ＩＣモジュール部１０には、Ｉ／Ｏインタフェース１１、ＣＰＵ１２、ＲＯＭ１３、ＲＡＭ１４、バイト書換型ＥＥＰＲＯＭ１５が内蔵されている。Ｉ／Ｏインタフェース１１は、Ｉ／Ｏライン１９を介してデータを送受するための入力回路であり、ＣＰＵ１２はこのＩ／Ｏインタフェース１１を介して、端末装置２００と交信することになる。ＲＯＭ１３内には、ＣＰＵ１２によって実行されるプログラムが記憶されており、ＣＰＵ１２はこのプログラムに基いて、第一ＩＣモジュール部１０を統括制御する機能を有する。ＲＡＭ１４は、ＣＰＵ１２がこのような統括制御を行う上での作業領域として使用されるメモリである。一方、バイト書換型ＥＥＰＲＯＭ１５は、第一ＩＣモジュール部１０に記録すべき本来のデータを格納するメモリである。ＩＣカード１００が端末装置２００と切り離されると、電源およびクロックの供給は停止する。このとき、ＲＡＭ１４内のデータは、電源供給の停止によりすべてが失われるが、バイト書換型ＥＥＰＲＯＭ１５は不揮発性メモリであるため、電源供給が停止した後もその記録内容はそのまま保持される。

【００２９】端末装置２００は、電気的アクセス手段２９によってフラッシュメモリー２０の接続端子４０に対するアクセスを行うこともできる。電気的アクセス手段２９は、上述した第一ＩＣモジュール１０とＩ／Ｏカードインターフェイスにより端末装置２００と交信するのと同様であり、フラッシュメモリー２０内にデジタル情報の記録を行う。この実施例に係るＩＣカード１００では、第一ＩＣモジュール部１０内のバイト書換型ＥＥＰＲＯＭ１５は８ＫＢの記録容量しかもたないのに対し、フラッシュメモリー２０には８ＭＢの情報記録が可能である。したがって、第一ＩＣモジュール部１０のみしか備えていないＩＣカードに比べれば、この２チップ型ＩＣカード１００には大量の情報を記録することが可能である。

【００３０】§２．改ざん防止機能を有する認証コードの生成方法

一般に、何らかの媒体に記録されているデータに対して、改ざんが行われるおそれがある場合、認証コードに基づいて改ざんの有無を判断する方法が知られている。すなわち、予め秘密の暗号化キーを用意しておき、この暗号化キーを用いて、もとのデータから一義的に導出される認証コードを生成する。そして、もとのデータとともにこの認証コードをチェックすることにより、改ざんの有無を判断ことができる。すなわち、データを認証コードとともに読出し、書込み時と同じ暗号化キーを用いて、読出したデータから一義的に導出される認証コードを生成し、この生成した認証コードと読出した認証コードとが一致するか否かを判断するのである。通常、両者は一致するはずであるから、万一、不一致が生じた場合

には、何らかの改ざんが行われたものと判断することができる。

【００３１】このような認証コードは、一般にＭＡＣ（Message Authentication Code ）と呼ばれている。ＭＡＣは、もとのデータから一義的に定まるデータであればどのようなデータを用いてもかまわないが、通常は、データ記録の冗長度をある程度に抑えるために、もとのデータの長さよりもかなり小さなＭＡＣが利用される。ＭＡＣに基づいて、逆にもとのデータを生成させる必要性はないので、もとのデータの情報量に対して、ＭＡＣの情報量がある程度小さくても問題はない。ただし、ＭＡＣはもとのデータの全般が関与する形で生成する必要がある。別言すれば、もとのデータの任意の１ビットに変化が生じた場合には、必ずＭＡＣ自身にも何らかの変化が現れるようにしておく必要がある。こうしておけば、いずれか１ビットでも改ざんされれば、ＭＡＣの照合が一致しなくなり、改ざんがあったことを認識することができる。

【００３２】このような条件を満たす認証コードＭＡＣの生成方法としては、もとのデータをブロック分割して取り扱う方法が知られている。たとえば、もとのデータをｎ個（ｎ≧２）のブロックに分割し、このｎ個のブロックにｍ個の暗号化キー（ｍ≧２）を加えた（ｎ＋ｍ）組のデータのすべてが関与した相互論理演算を行い、もとのデータのデータ長よりも短い認証コードＭＡＣを生成するのである。

【００３３】この方法の具体例を図３を参照しながら説明する。いま、図３の上部に示したように、所定の長さをもった「１区切りのデータ」に対して認証コードＭＡＣを生成する場合を考える。この場合、この「１区切りのデータ」を複数ｎ個のブロックに分割する。この例では、１つのブロックのデータ長が８バイトとなるような分割が行われている。続いて、所定の暗号化キーＫ（例えば、８バイトのデータ）を用いて、暗号化手段３１によってブロック１に対する暗号化処理を行い、その結果としてブロック１’を得る。暗号化手段３１において実行する暗号化処理は、ブロック１と暗号化キーＫとを用いた論理演算であればどのようなものでもかまわない。いずれにせよ、得られるブロック１’は、ブロック１と暗号化キーＫとが特定されれば一義的に定まるデータになる。次に、演算器３２によって、ブロック１’とブロック２との排他的論理和をとり、ブロック２’を求め、続いて、演算器３３によって、ブロック２’とブロック３との排他的論理和をとり、ブロック３’を求める。以下、同様に、ブロックｉ’とブロック（ｉ＋１）との排他的論理和をとり、ブロック（ｉ＋１）’を得る処理をｉ＝ｎ－１になるまで繰り返し実行し、ブロックｎ’を求めれば、このブロックｎ’が生成すべき認証コードＭＡＣとなる。この例では、もとの「１区切りのデータ」が（８×ｎ）バイトの長さであったのに対して、得られた認証コードｍａｃは８バイトの長さになる。

【００３４】このような方法で生成された認証コードＭＡＣは、もとの「１区切りのデータ」と暗号化キーＫとに基づいて一義的に導出されるコードであり、もとのデータ内のいずれか１ビットでも変更されると、異なった値をとる。なお、図３に示した認証コードＭＡＣの生成方法は、一例を示したものであり、本発明は、このような認証コードＭＡＣの生成方法に限定されるものではない。例えば、ブロック２’と暗号化キーＫとに基づいてブロック３’を得るようにしてもよいし、演算器３２として他の論理演算を行うようにしてもよいし、暗号化キーＫ１、Ｋ２、・・・と複数のキーを用いるようにしてもよい。要するに、与えられたデータと予め用意した暗号化キーとに基づいて一義的に定まるようなコードであれば、どのようなコードを認証コードＭＡＣとして用いてもかまわない。

【００３５】§３．セキュリティを有する２チップ型ＩＣカード

続いて、本発明のセキュリティを有する２チップ型ＩＣカードの構成と、このＩＣカードの第２ＩＣモジュール部としてのフラッシュメモリーに対するデータの書込処理および読出処理を説明する。図４は、本発明の一実施例に係る２チップ型ＩＣカード１００を端末装置２００に接続し、アクセスを行っている状態を示すブロック図であり、そのハードウエア構成は、図２において述べた２チップ型ＩＣカードと同様である。ただ、ＲＯＭ１３内にＭＡＣ生成ルーチンが付加され、バイト書換型ＥＥＰＲＯＭ１５内に暗号化キーＫが記録されている点が異なり、また、フラッシュメモリー２０内に記録される「１区切りのデータ」には、認証コードＭＡＣが付加される点が異なる。

【００３６】はじめに、図５の流れ図を参照しながら、この図４に示す２チップＩＣカード１００についてのフラッシュメモリー２０へのデータ書込処理の手順を説明する。なお、この流れ図において、ステップＳ１１、Ｓ１２、Ｓ１６は端末装置２００側でフラッシュメモリー２０への記録すべき記録対象データを用意する。この記録対象データは、図３における「１区切りのデータ」に対応するものである。認証コードＭＡＣの長さに比べて、「１区切りのデータ」の長さが長ければ、それだけ認証の精度が低下するので、この「１区切りのデータ」の長さは、必要な認証精度を考慮の上、適宜設定しておくようにする。

【００３７】続くステップＳ１２では、ステップＳ１１で用意したデータをＭＡＣ生成コマンドとともに第一ＩＣモジュール部１０へと転送する。このように、「コマンド」の形式で、端末装置２００から第一ＩＣモジュール部１０へデータを転送するのは、端末装置２００と第一ＩＣモジュール部１０との間の交信が、「コマンド」とそれに対する「レスポンス」という形で行われるから

である。すなわち、端末装置２００からＣＰＵ１２に対して所定の「コマンド」を与えると、ＣＰＵ１２はこの「コマンド」を解釈し、ＲＯＭ１３内に用意されているこのコマンドに対応したルーチンを実行し、その結果を、端末装置２００に対して「レスポンス」として返送することになる。例えば、バイト書換型ＥＥＰＲＯＭ１５内の所定のファイルに書き込みを行う場合には、「書込コマンド」とともに書込対象となるデータをＣＰＵ１２に与え、ＣＰＵ１２による「書込コマンド」の実行という形式で書込処理が行われることになる。逆に、バイト書換型ＥＥＰＲＯＭ１５内の所定のファイルからデータの読出しを行う場合は、所定の「読出コマンド」をＣＰＵ１２に与え、ＣＰＵ１２による「読出コマンド」の実行という形式で読出処理が行われることになる。このように、第一ＩＣモジュール１０内において「コマンド」の実行が終了すると、実行した「コマンド」に対する「レスポンス」が外部に対して返送される。例えば、「書込コマンド」を与えた場合には、書込処理が支障なく実行されたか否かを示す「レスポンス」返送され、「読出コマンド」を与えた場合には、読出対象となったデータがレスポンスという形で返送されることになる。そこで、ステップＳ１２では、認証コードＭＡＣを生成する指示を与える「ＭＡＣ生成コマンド」とともに、ステップＳ１１で用意した記録対象データ（図３の「１区切りのデータ」に対応するデータ）を第一ＩＣモジュール部１０へ与えている。

【００３８】第一ＩＣモジュール部１０は、このようなコマンドを解釈し、ＲＯＭ１３内に用意されたＭＡＣ生成ルーチンを利用して、次のような処理を実行する。まず、この実施例では、ＭＡＣ生成ルーチンの実質的な処理に入る前に、ステップＳ１３において、現在接続されている端末装置２００が正規の端末装置として認証済みであるか否かがチェックされる。通常、ＩＣカード１００を端末装置２００に挿入し、両者を電気的に接続すると、相互に相手方が正しいものであるか否かを確認する相互認証処理が実行される。このような相互認証処理の具体的な方法については、既に公知の技術であるのでここでは説明を省略するが、この相互認証の結果、ＩＣカード１００側が相手（端末装置２００）を正しいものと認証すると、通常は、ＲＡＭ１４内の「相手が正規の端末装置であることを示すフラグ」をセットする処理が行われる。この実施例では、ステップＳ１３において、まずこのフラグがセットされていることを確認した後、ＭＡＣ生成ルーチンを実行するようにしている。これは、セキュリティを更に向上させるための配慮であり、そのメリットについては後述する。

【００３９】さて、ステップＳ１３において、現在接続されている端末装置２００が正規の端末装置であることが確認できたら、続くステップＳ１４において、認証コードＭＡＣを生成する処理が行われる。すなわち、端末装置２００からコマンドとともに与えられた記録対象データ（図３の「１区切りのデータ」とバイト書換型ＥＥＰＲＯＭ１５内に用意されている暗号化キーＫとに基づいて一義的に導出される何らかのコードが生成される。この実施例では、図３に示す方法によって、認証コードＭＡＣが生成される。こうして認証コードＭＡＣが生成されたら、これをステップＳ１５においてレスポンスとして端末装置２００側へ返送する。

【００４０】結局、端末装置２００側から上述の処理を見ると、ステップＳ１２において、コマンドとともに記録対象データをＩ／Ｏライン１９を介して転送すると、ステップＳ１５において、同じくＩ／Ｏライン１９を介してレスポンスが得られたことになり、このレスポンスには、転送した記録対象データについての認証コードＭＡＣが含まれていることになる。そこで、端末装置２００は、ステップＳ１６において、用意した記録対象データ（「１区切りのデータ」）に、レスポンスとして戻された認証コードＭＡＣを付加し、これを電気的アクセス手段２９を介してフラッシュメモリー２０内に書込む処理を行う。かくして、図４に示すように、フラッシュメモリー２０内には、「１区切りのデータ」が認証コードＭＡＣとともに書込まれることになる。

【００４１】なお、ステップＳ１３において、現在接続されている端末装置２００が正規の端末装置ではないと判断された場合、すなわち、相互認証処理が正常に完了したことを示すフラグがＲＡＭ１４内にセットされていなかった場合は、ステップＳ１７において、エラーレスポンスが返送される。したがって、たとえば、不正な端末装置によってＩＣカード１００と交信し、この不正な端末装置からＭＡＣ生成コマンドを与えたとしても、ＩＣカード１００からはエラーレスポンスが戻ることになり、認証コードＭＡＣを得ることはできない。したがって、不正な端末装置を用いて、特定のデータについての認証コードＭＡＣを知得するような不正行為は拒絶され、十分なセキュリティを確保することが可能になる。もちろん、ステップＳ１３の判断処理は、本発明を実施する上で必要不可欠の処理ではないが、実用上、十分なセキュリティを確保する上では、この処理を実行するのが好ましい。

【００４２】続いて、図６の流れ図を参照しながら、図４に示す２チップ型ＩＣカード１００についてのフラッシュメモリー２０からのデータ読出処理の手順を説明する。なお、この流れ図において、ステップＳ２１、Ｓ２２は端末装置２００において行われる処理であり、ステップＳ２３～Ｓ２７はＩＣカード１００において行われる処理である。まず、ステップＳ２１において、フラッシュメモリー２０から電気的的アクセス手段２９を介して、ＭＡＣ付データの読出しが行われる。すなわち、図４のフラッシュメモリー２０に示す「１区切りのデータ」と認証コードＭＡＣとが１組のデータとして、端末

装置２００側に読み出されることになる。

【００４３】続くステップＳ２２では、ステップＳ２１で読出したデータをＭＡＣ照合コマンドとともに第一ＩＣモジュール部１０へと転送する。第一ＩＣモジュール部１０は、このようなコマンドを解釈し、ＲＯＭ１３内に用意されたＭＡＣ生成ルーチンを利用して、次のような処理を実行する。まず、この実施例では、ＭＡＣ生成ルーチンの実質的な処理に入る前に、ステップＳ２３において、現在接続されている端末装置２００が正規の端末装置として認証済みであるか否かがチェックされる。これは、前述したステップＳ１３の処理と同様である。現在接続されている端末装置２００が正規の端末装置であることが確認できたら、続くステップＳ２４において、認証コードＭＡＣを照合する処理が行われる。すなわち、端末装置２００からコマンドとともに与えられたデータを、本来のデータ部分と認証コードＭＡＣの部分とに分割し、本来のデータ部分（図３の「１区切りのデータ」に相当）とバイト書換型ＥＥＰＲＯＭ１５内に用意されている暗号化キーＫとに基づいて、認証コードＭＡＣを生成する。この実施例では、図３に示す方法によって、認証コードＭＡＣが生成される。こうして認証コードＭＡＣが生成されたら、この生成された認証コードＭＡＣと、端末装置２００から与えられた認証コードＭＡＣと、が一致するか否かを判断する。

【００４４】フラッシュメモリー２０内に記録されていた情報が、書込み時のままであれば、ステップＳ２５における照合結果は一致を示すはずであるが、何らかの改ざんが行われていた場合には不一致を示すことになる。そこで、照合結果が一致すれば、ステップＳ２６において正常レスポンスを返送し、不一致であれば、ステップＳ２７においてエラーレスポンスを返送する。端末装置２００側では、このレスポンスに基づいて、フラッシュメモリー２０から読出したデータに対する改ざんの有無を認知することができるすなわち、正常レスポンスが得られた場合には、読出したデータを正しいデータとして取り扱うことができ、エラーレスポンスが得られた場合には、読出したデータには不正な改ざんが行われているとの認識のもとにしかるべき取扱を行うことができる。

【００４５】なお、ステップＳ２３において、正規の端末装置ではないと判断された場合、すなわち、相互認証処理が正常に完了したことを示すフラグがＲＡＭ１４内にセットされていなかった場合は、ステップＳ２７において、エラーレスポンスが返送される。したがって、たとえば、不正な端末装置によってＩＣカード１００と交信し、この不正な端末装置からＭＡＣ照合コマンドを与えたとしても、ＩＣカード１００からはエラーレスポンスが戻ることになり、照合結果を得ることはできない。したがって、不正な端末装置を用いて、特定のデータと認証コードＭＡＣとの組み合わせについての照合結果を知得するような不正行為は拒絶され、十分なセキュリティを確保することが可能になる。もちろん、ステップＳ２３の判断は、本発明を実施する上で必要不可欠の処理ではないが、実用上、十分なセキュリティを確保する上では、この処理を実施するのが好ましい。

【００４６】§４．本発明の変形例

最後に、本発明の変形例を示す。図７は、これまで述べてきた本発明のＩＣカード１００を用いた取引システムの一例を示すブロック図である。ここでは、２つの端末装置に２０１と２０２と４枚のＩＣカード１０１～１０４とを用いた非常に単純なモデルを示してあるが、実際には、より多くの端末装置およびＩＣカードが用いられる。このようなシステムでは、４枚のＩＣカード１０１～１０４は、端末装置２０１、２０２のいずれにも接続可能である。たとえば、第１のＩＣカード１０１のフラッシュメモリー、第１の端末装置２０１を用いて所定のデータを書き込んだ場合、このデータは、第２の端末装置２０２によっても何ら支障なく読みだすことができる。なぜなら、認証コードＭＡＣを生成するために用いられる暗号化キーＫ１は、ＩＣカード１０１内に用意されており、かつ、ＭＡＣ生成ルーチンもＩＣカード１０１内に用意されているので、どの端末装置を用いても同じ結果が得られるからである。したがって、本発明は、図７に示すような取引システムに何ら支障なく適用可能である。

【００４７】図８は、図７に示す取引システムに、更に第３の端末装置２０３および第４の端末装置２０４を付加したものである。ここで、第３の端末装置２０３および第４の端末装置２０４は、いずれもホストコンピュータ３００に接続されている。図７に示す第１の端末装置２０１および第２の端末装置２０２は、いずれもいわゆる「スタンドアロン型」のものであり、ホストコンピュータ３００には接続されていない。これに対し、図８に示す第３の端末装置２０３および第４の端末装置２０４は、いずれもいわゆる「ネットワーク型」のものであり、ホストコンピュータ３００に対してオンライン接続されている。

【００４８】実社会における取引システムでは，しばしばこのようなに「スタンドアロン型」の端末装置と「ネットワーク型」の端末装置を混在させた形態が見られる。たとえば，銀行システムの場合，各支店等の比較的大規模な営業所には「ネットワーク型」の端末装置を設け、駅や百貨店の一角には「スタンドアロン型」の端末装置を設置するような利用形態が考えられる。本発明における「端末装置」という文言は、「スタンドアロン型」の装置と「ネットワーク型」の装置とを含んだ広い概念で用いられており、本発明は，図７の取引システムにも図８の取引システムにも、いずれにも適用可能である。

【００４９】ただ、図８のような「ネットワーク型」の端末装置を含むシステムにも適用する場合、ＭＡＣ生成

15

処理やＭＡＣ照合処理をホストコンピュータ３００側で行うことも可能である。即ち，各ＩＣカード１０１～１０４のＲＯＭ内に用意されたＭＡＣ生成ルーチンおよび第一ＩＣモジュールのバイト書換型ＥＥＰＲＯＭ内に用意された暗号化キーＫ１，Ｋ２，Ｋ３，ｋ４を、ホストコンピュータ３００内に用意しておくようにすれば、前述の実施例においてＩＣカード内で実施していたＭＡＣ生成処理（ステップＳ１３）やＭＡＣ照合処理（ステップＳ２４）をホストコンピュータ３００側で実行することも可能になる。

【００５０】このような処理をホストコンピュータ３００側で行うと，処理時間を短縮出来るとういメリットが得られる。即ち、個々のＩＣカードに内蔵されたＣＰＵと、ホストコンピュータ３００内のＣＰＵとを比較すると、両者のコストを比較すれば明らかなように、前者の演算処理能力は、後者の演算処理能力に比べれば非常に劣るものである。このため、例えば図３に示すような演算処理をＩＣカード側のＣＰＵに実行させればかなりの時間が必要になるのに対し、ホストコンピュータ３００側のＣＰＵに実行させれば一瞬に演算は完了する。また、これらの処理をＩＣカード側のＣＰＵに実行させるためには、端末装置からＩ／Ｏライン１９を介してコマンドという形式でデータを転送する必要があり、この転送作業にもある程度の時間が必要になり、ＩＣカード側での処理をさらに遅くする要因となっている。そこで，図８に示す端末装置２０３，２０４のように、ホストコンピュータ３００に対してオンライン接続されている端末装置を用いてＩＣカード１００をアクセスしている場合には、ＭＡＣ生成処理やＭＡＣ照合処理を、ＩＣカード側で行う代わりに、ホストコンピュータ３００側で行うと、全体の処理時間が短縮される。ただ，ＭＡＣ生成ルーチンや個々のＩＣカードについての暗号化キーＫ１～Ｋ４をホストコンピュータ３００内に用意するため、十分なセキュリティを確保する必要がある。また、ホストコンピュータ３００内でＭＡＣ生成処理やＭＡＣ照合処理を実行する前に、ホストコンピュータ・端末装置・ＩＣカードの三者間において、互いに相手が正規のものであることを確認する相互認証がおこなわれていることを確認するようにすれば、不正アクセスに対しても十分なセキュリティ確保が実現できる。

【００５１】以上、本発明を図示する実施例に基づいて説明したが、本発明はこれらの実施例に限定されるものではなく、この他にも種々の態様で実施可能である。たとえば、上述の実施例では、第二ＩＣモジュール部にフラッシュメモリーを例にとって説明を行ったが、バイト書換型ＥＥＰＲＯＭを用いてもよく、また、その逆に第一ＩＣモジュール部内のバイト書換型ＥＥＰＲＯＭにフラッシュメモリーを用いてもよいものである。さらに、バイト書換型ＥＥＰＲＯＭはその最小単位のビット単位にて書換・消去可能なビット書換型ＥＥＰＲＯＭとして

16

ももちろん構わないものである。

【００５２】

【発明の効果】以上のとおり本発明によれば、ＣＰＵを有するＩＣモジュールと、それ以外のカード表面に電気的に消去・再書き込み可能な不揮発性メモリからなる別のＩＣモジュールとを搭載したＩＣカードとすることにより、その双方のＩＣモジュールに情報を記録することのできる、大容量の情報記録が可能で、処理速度が速く、かつ表面物性に優れた携帯可能情報記録媒体を提供するとともに、その記録情報に対するセキュリティの非常に高い、電気的に消去・再書き込み可能な不揮発性メモリからなるＩＣモジュールに記録された情報の改ざんに対する有効な対策をも実現できる。

【図面の簡単な説明】

【図１】ＩＣモジュール部１０およびフラッシュメモリー２０を搭載した２チップ型ＩＣカードの外観図である。

【図２】図１のＩＣカード１００を端末装置２００に接続し、アクセスを行っている状態を示すブロック図である。

【図３】認証コードＭＡＣの生成方法の一例を示す図である。

【図４】本発明の一実施例に係る２チップ型ＩＣカード１００を端末装置２００に接続し、アクセスを行っている状態を示すブロック図である。

【図５】図４に示す２チップ型ＩＣカード１００についてのフラッシュメモリー２０へのデータ書込処理の手順を説明する流れ図である。

【図６】図４に示す２チップ型ＩＣカード１００についてのフラッシュメモリー２０からの読出処理の手順を説明する流れ図である。

【図７】本発明に係るＩＣカードとスタンドアロン型端末装置を用いた取引システムの一例を示すブロック図である。

【図８】本発明に係るＩＣカードとネットワーク型端末装置を用いた取引システムの一例を示すブロック図である。

【符号の説明】

１０　ＩＣモジュール部
１１　Ｉ／Ｏインタフェース
１２　ＣＰＵ
１３　ＲＯＭ
１４　ＲＡＭ
１５　バイト書換型ＥＥＰＲＯＭ
１９　Ｉ／Ｏライン
２０　フラッシュメモリー
２９　電気的アクセス手段
３０　接触端子
３１　暗号化手段
４０　接触端子

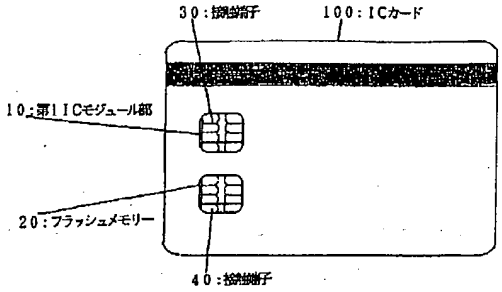
17

１００～１０４
２００～２０４

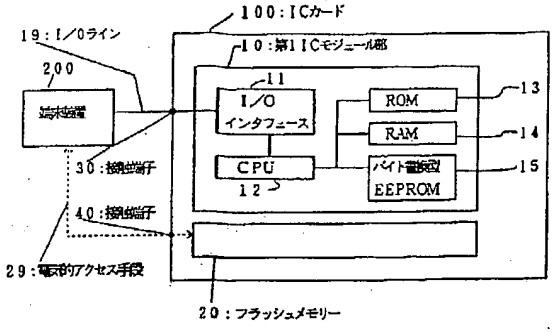
18

３００

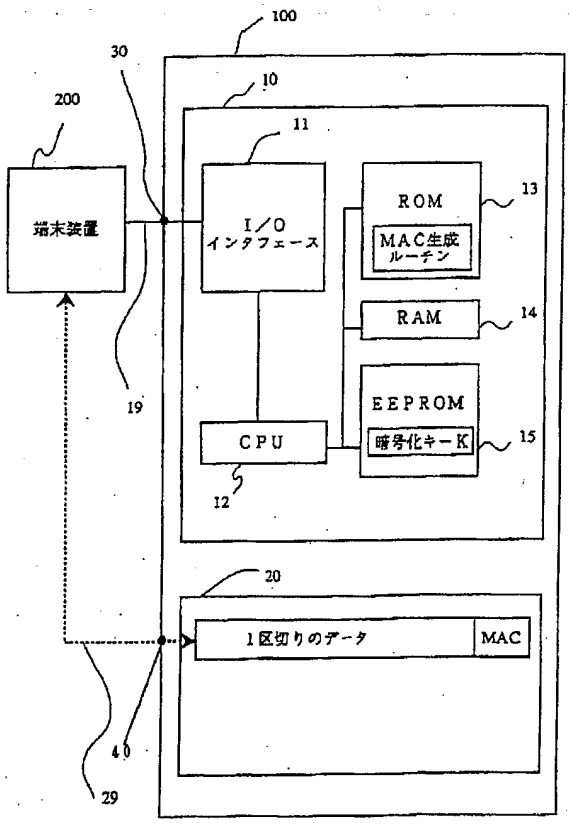
【図１】



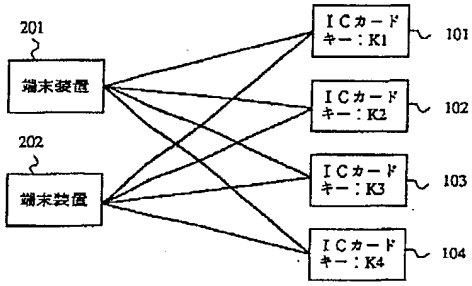
【図２】



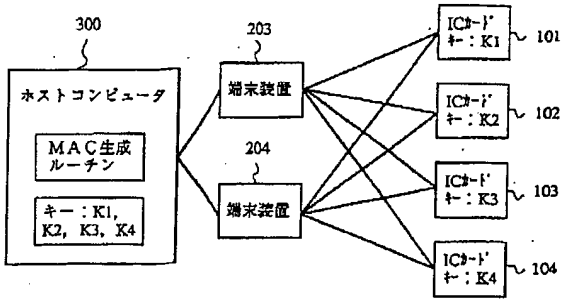
【図４】



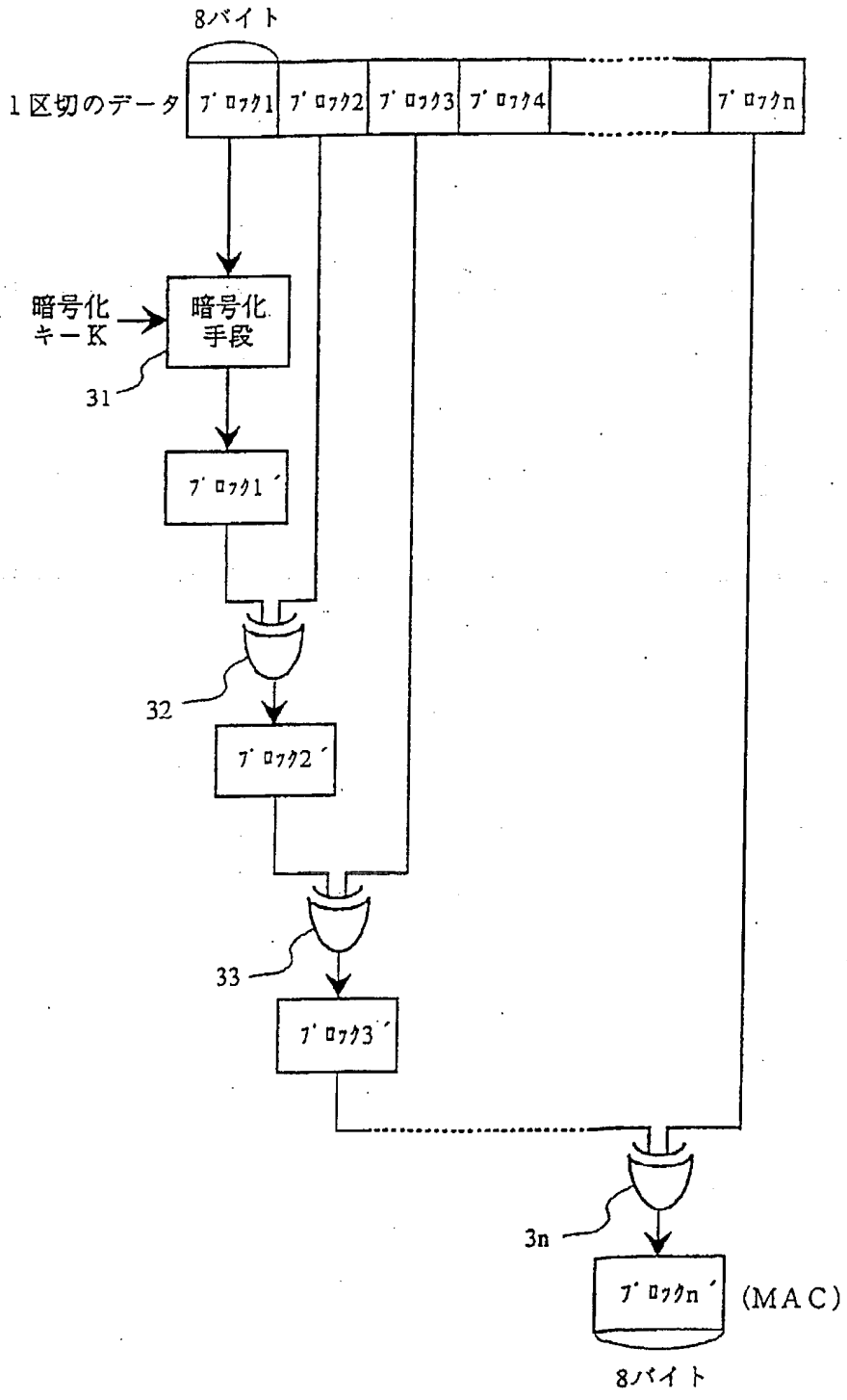
【図７】



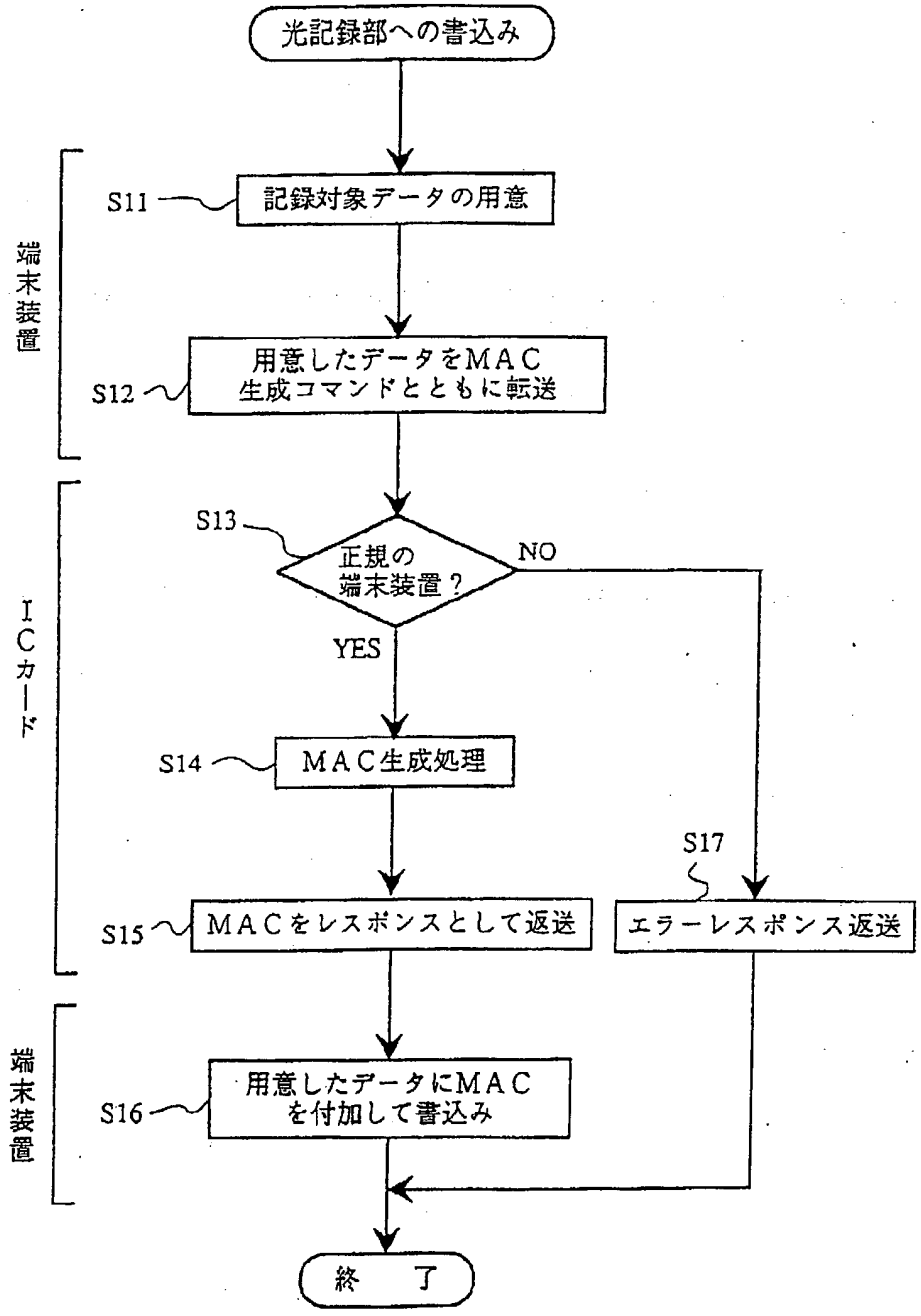
【図８】



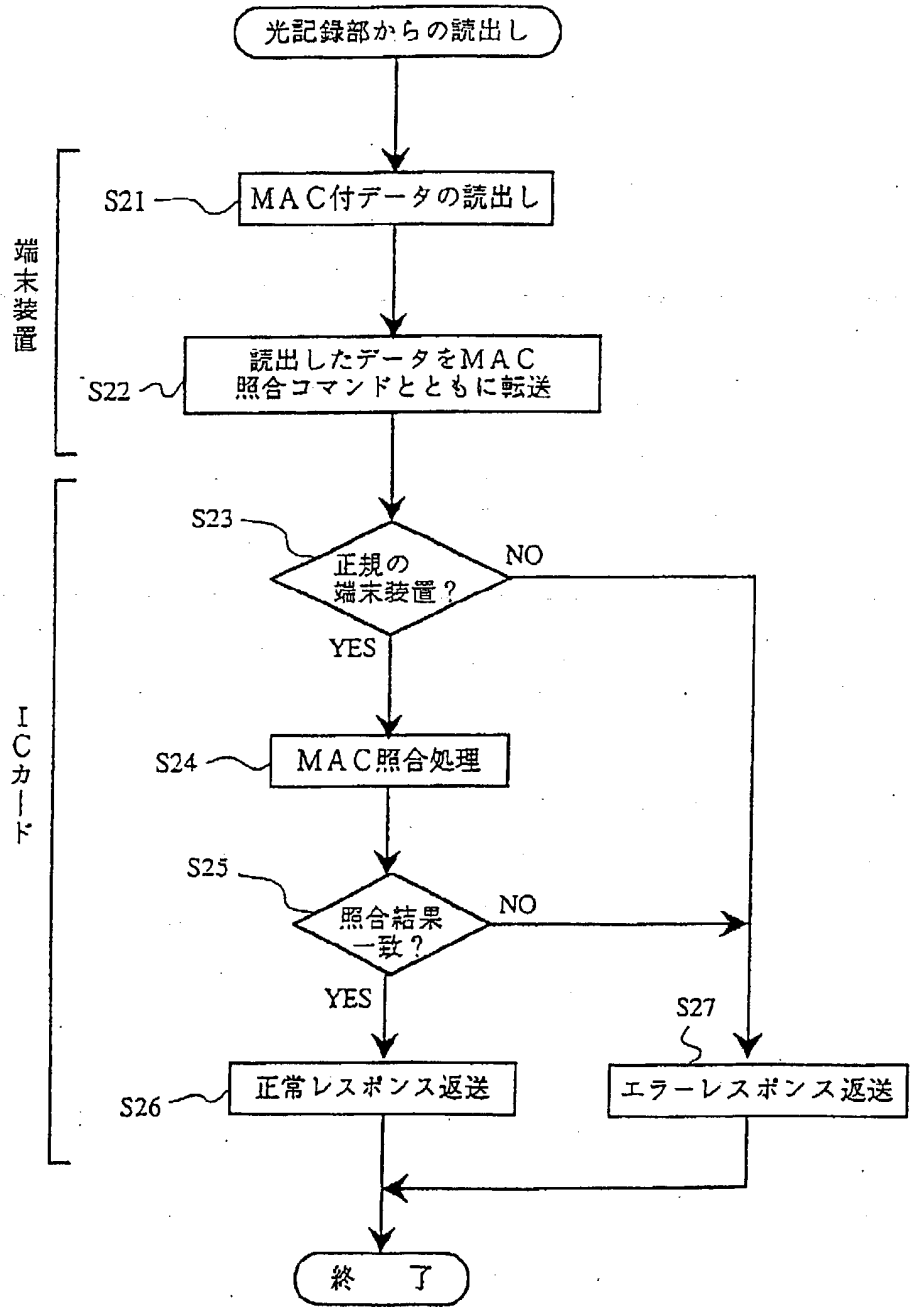
【図３】


8バイト
1区切のデータ
ﾌﾞﾛｯｸ1
ﾌﾞﾛｯｸ2
ﾌﾞﾛｯｸ3
ﾌﾞﾛｯｸ4
ﾌﾞﾛｯｸn
暗号化
キーK
暗号化
手段
31
ﾌﾞﾛｯｸ1´
32
ﾌﾞﾛｯｸ2´
33
ﾌﾞﾛｯｸ3´
3n
ﾌﾞﾛｯｸn´
(MAC)
8バイト

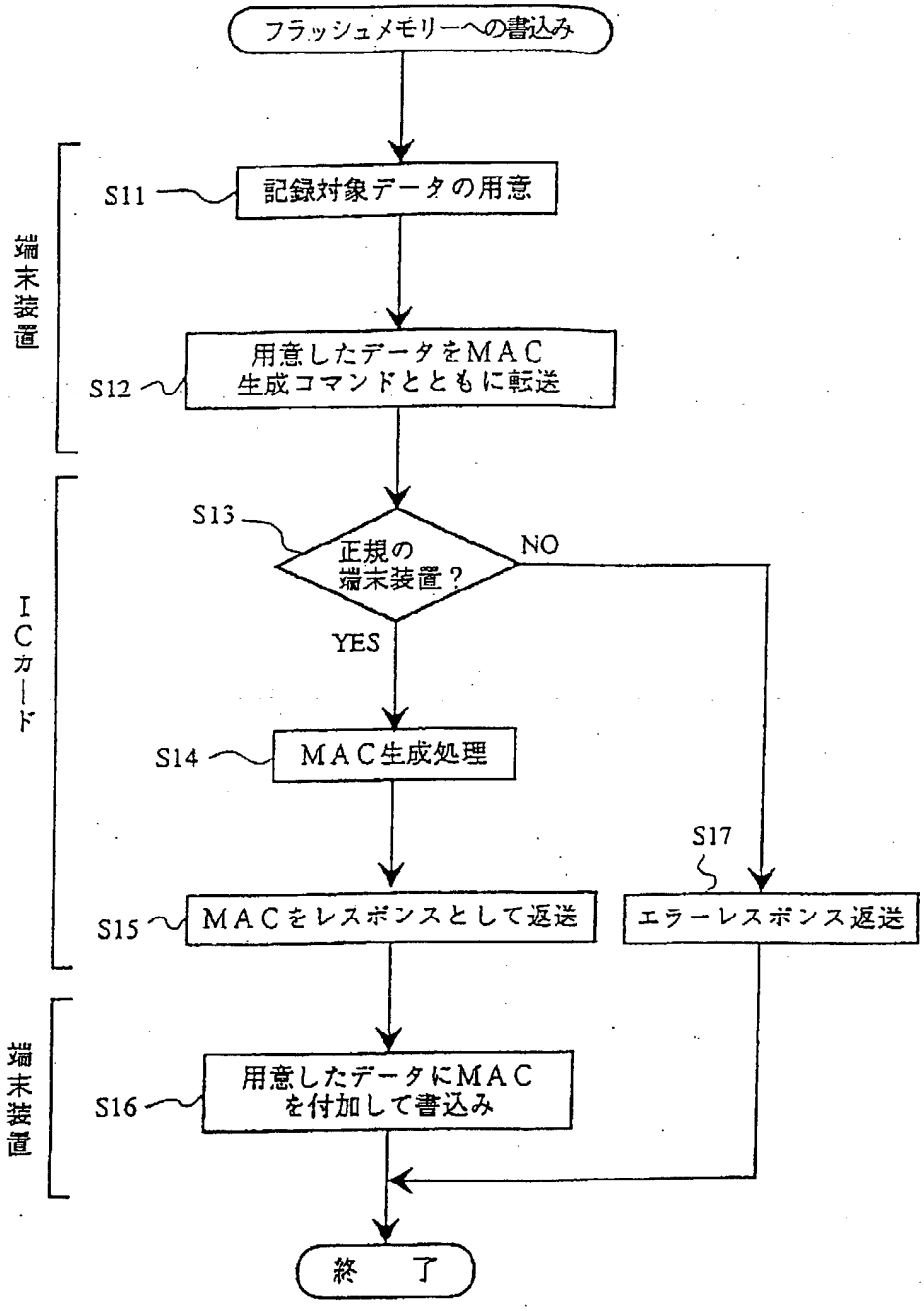
【図５】


光記録部への書込み
端末装置
S11
記録対象データの用意
S12
用意したデータをＭＡＣ
生成コマンドとともに転送
ＩＣカード
S13
正規の
端末装置？
NO
YES
S14
ＭＡＣ生成処理
S17
S15
ＭＡＣをレスポンスとして返送
エラーレスポンス返送
端末装置
S16
用意したデータにＭＡＣ
を付加して書込み
終　了

【図６】

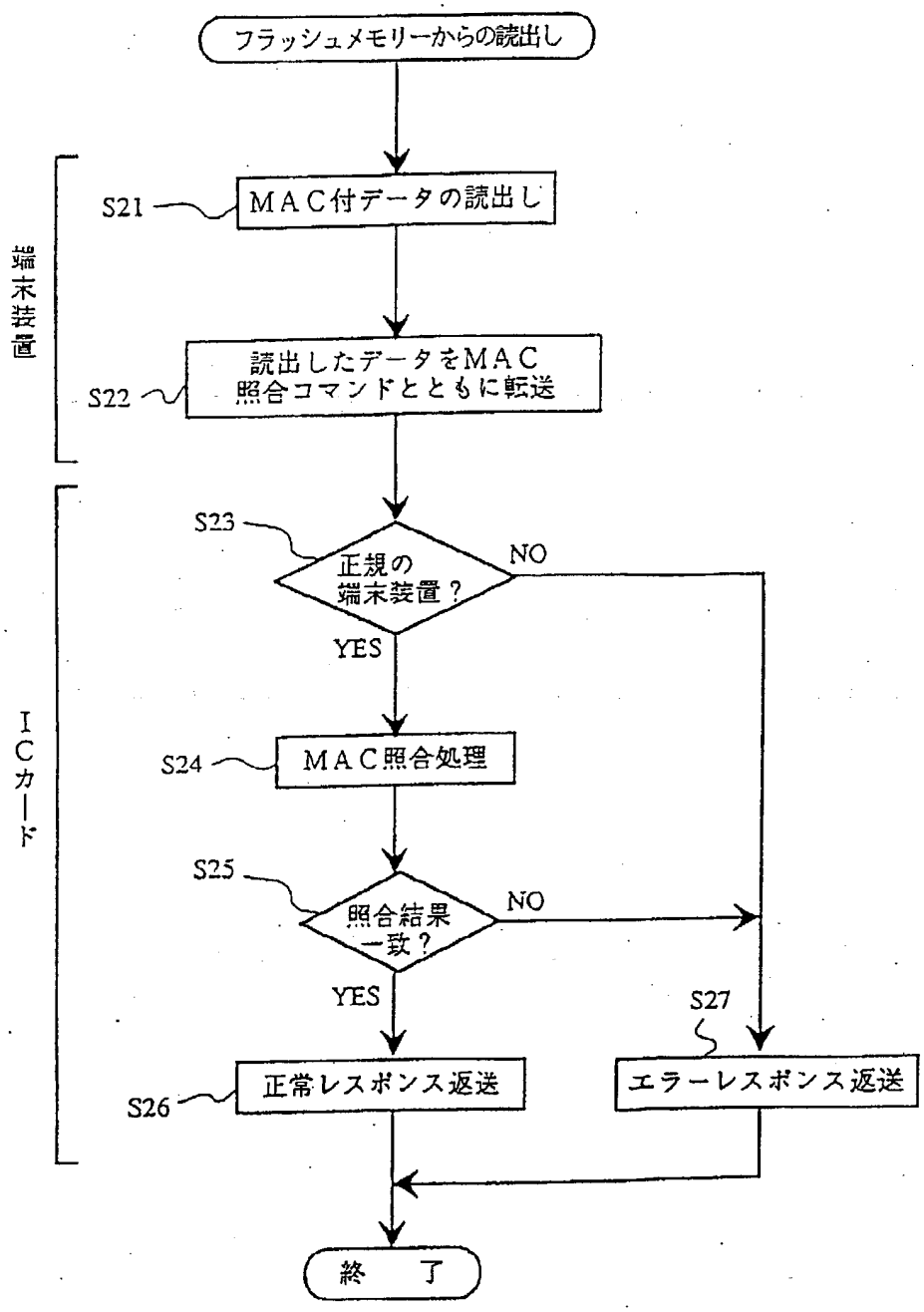


【手続補正書】
【提出日】平成９年３月１８日
【手続補正１】
【補正対象書類名】図面
【補正対象項目名】図５
【補正方法】変更
【補正内容】
【図５】



【手続補正２】
【補正対象書類名】図面
【補正対象項目名】図６

【補正方法】変更
【補正内容】
【図６】


フラッシュメモリーからの読出し
端末装置
S21
ＭＡＣ付データの読出し
S22
読出したデータをＭＡＣ照合コマンドとともに転送
ＩＣカード
S23
正規の端末装置？
NO
YES
S24
ＭＡＣ照合処理
S25
照合結果一致？
NO
YES
S26
正常レスポンス返送
S27
エラーレスポンス返送
終　了